GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:6228
ANSWERED ON:12.04.2017
Promotion of e-payment
Kateel Shri Nalin Kumar;Suresh Shri Doddaalahalli Kempegowda

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

Will the Minister of ELECTRONICS & INFORMATION TECHNOLOGY be pleased to state: -
(a) whether the Government is aware that the consumer does not browse the Internet due to constant hassles of connectivity and other bothering factors;
(b) if so, the details thereof and the reasons therefor;
(c) whether the Government is aware that electronic payment is not so popular in the country due to increasing threat of fraud played by hackers; and
(d) if so, the details of steps being taken to prevent fraud and infuse confidence among people to use electronic payment

Answer

(a) and (b): As per the TRAI data there is a trend of growth of Internet subscribers. The number of Internet subscriber base at the end of September 2016 was 367.48 million & total No. of Internet subscriber base at the end of December 2016 was 391.50 million, which shows that there is addition of 24.02 million or 240.2 Lakhs internet subscribers in the country) during this period. Hence connectivity does not seem to be an issue for browsing internet.
(c) and (d): The data received from RBI shows only few cases for unusual cyber security incidents reported, which shows that electronic payment is popular in the country.

RBI data: As of February 28, 2017, the details of the incidents reported by bank (since issuance of RBI circular No. DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016 on Cyber Security Framework in Banks, wherein banks have been advised to report all unusual cyber security incidents to RBI within 2 - 6 hours of detection) are as given under:

Sl No Type of Incidents Total no of incidents reported
1 Ransom ware 7
2 Distributed Denial of Service (DDos) 2
3 Phishing Attacks 6
4 Rogue Mobile Application 6
5 Card Skimming 3
6 Virus/Malware 13
Further, the details of frauds related to Credit/ ATM / Debit cards & Net Banking reported by banks during last three years and current year (From April 01, 2013 to December 31, 2016) and extent of losses occurred due to such incidents are as given below:
(i) Details of frauds reported in Credit Cards/ ATM/Debit Cards and Internet Banking Categories (Amount in Lakh `)
Financial Year Credit Cards ATM/ Debit Cards Internet Banking Total (All three categories)
No. of Frauds Amount No. of Frauds Amount No. of Frauds Amount No. of Frauds Amount
2013-14 7890 5481.59 1307 823.17 303 1495.83 9500 7800.59
2014-15 10382 4231.97 2498 1385.98 203 2445.8 13083 8063.75
2015-16 9849 4597.79 6585 3126.85 34 175.31 16468 7899.95
June, September, Dec.Quarter 2016 4557 2156.78 4064 1900.8 68 158.18 8689 4215.76
Source: FMR2 submitted by banks (All Frauds − including amount involving below `1.00 Lakh)
(ii) Details of frauds in Credit cards/ATM/Debit cards & internet banking categories (Fraud cases of Rs.1 lakh and above) and Extent of loss incurred are as given below:
Amount in Lakh (`) - Source: FMR1
Financial Year No. of cases reported Total Amount involved Extent of Loss to banks
2013-14 978 5451.77 3225.31
2014-15 845 5169 1848.5
2015-16 1190 4019.12 2702.26
June, September & December Quarter 2016 1081 3501.88 2635.43
Total 4094 18141.77 10411.5

Further the Government has taken the following steps to prevent fraud and infuse confidence among people to use electronic payments:
i. All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by Indian Computer Emergency Response Team (CERT-In) through the Reserve Bank of India to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.
i. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.
ii. Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/

Departments of Central Government, State Governments and their organizations and critical sectors.

iii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 11 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 110 organisations from different sectors including Finance sector. The last drill was conducted on 30th September 2016 in coordination with Reserve Bank of India for Finance Sector.

iv. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and mobile phones on regular basis. 21 advisories have also been issued regarding safeguards for users and institutions to secure digital payments.

v. It has been mandated that all government websites should be hosted on infrastructure of National Informatics Centre (NIC) or any other secured government infrastructure in the country. NIC which hosts the government websites is continuously engaged in upgrading and improving the security posture of its hosting infrastructure.

vi. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also. The Indian Computer Emergency Response Team (CERT-In) has empanelled 32 security auditing organizations to support and audit implementation of Information Security Best Practices.

vii. CERT-In is regularly tracking the hacking of websites and alerts the website owners concerned to take actions to secure the websites to prevent recurrence. CERT-In also issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

viii. Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for common users.

ix. MeitY has formulated draft rules for security of pre-paid payment instruments. The draft rules have been published on MeitY website inviting public comments.

x. The IT Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

xi. Ministry of Electronics & Information Technology (MeitY) has recently notified the scheme for evaluating any Department, body or agency of the Central Government or a State Government to notify them as Examiner of Electronic Evidence under Section 79A of IT Act, 2000.

xii. CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 18 such training programs were conducted covering 580 participants during the year 2016. In addition 2 workshops on security of digital payments systems have been conducted for stakeholder organisations covering 110 participants.

xiii. Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of cyber crime cases.

xiv. With respect to the banking sector, in order to focus more attention on IT related matters, Reserve Bank of India (RBI) has taken various action which includes :

a. RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.

b. The Bank has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security including inter alia advising banks to report all unusual cyber security incidents to RBI within 2-6 hours of detection.

c. RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This examination report has a special focus on cyber security. The reports have been issued to the banks for remedial action.

d. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.

e. Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.

f. RBI also has set up an IT subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.

g. RBI has issued circular on 09th December 2016 in Security and Risk mitigation measures for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

h. In addition, RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

i. RBI vide Circular No. DBS.CO.ITC.BC.No. 6 /31.02.008/2010-11 dated April 29, 2011 indicated that banks may consider insurance to transfer risk to a third party, however taking due care regarding certainty of payments in the event of disruptions.